Chapter VIII

Smart Cards for Security and Assurance

Konstantinos Markantonakis, University of London, UK
Keith Mayes, University of London, UK
Fred Piper, University of London, UK

Abstract

When designing and implementing a system that handles sensitive or valuable information, there can be few discussions that do not include some reference to ensuring adequate security. At a strategic level there will be high level requirements for security that will safeguard the system, which must ultimately translate to practical solutions and physical implementations. This chapter focuses on the technical implementation of security requirements and, in particular, the use of smart cards as trusted security tokens. In particular, it examines the significance of tamper resistance by exploring the different hardware and software platforms in relation to smart card attacks. It also highlights certain issues around the deployment of smart card technology in the financial industry.
Introduction

When designing and implementing a system that handles sensitive or valuable information, there can be few discussions that do not include some reference to ensuring adequate security. At a strategic level there will be high level requirements for security that will safeguard the system, which must ultimately translate to practical solutions and physical implementations. This chapter focuses on the technical implementation of security requirements and, in particular, the use of smart cards as trusted security tokens. One of the major objectives is to explain the need for tamper resistance in consumer security tokens and to describe the fine balance between the sophisticated attacks and countermeasures. However, to put this aspect in context, the chapter concludes with a discussion on the many other important issues involved, based around an example of a smart card system migration.

Smart Cards: How We Came to Need Tamper-Resistant Security

The possession and use of personal security, identity, and entitlement tokens goes back many years and certainly was not waiting for electronics and technology to come along. A physical door key is an age-old example of a personal security token that enables access. In authentication terminology, it is clearly “something you have,” but in some circumstances, it also requires “something you know,” basically because you need to find the door that it will fit. Physical keys can of course be legitimately copied or fraudulently reproduced via more dubious means. Unfortunately, a basic lock has no means of rejecting forgeries, as it cannot differentiate them from authentic keys. Like many security problems, determining authenticity is not new, and, for this reason, token solutions were widely used in the past. In medieval times the use of seals was increasingly popular (Ashdon-Hill, 2005). If a nobleman wanted to prove that he had actually sent a letter, then he could sign it and add some wax with an imprint of his personal token, that is, a customised seal. The resulting wax seal could later be checked for authenticity. If the seal had to be broken to read the letter, then it also served as some proof of integrity and confidentiality, that is, that the contents had not be modified or leaked to a third party. In the case of the nobleman’s seal, there may have been implied rights and entitlements because of his rank, but this would not be the case in a solution for all citizens. By contrast, during World War II, there was widespread use of food ration books (Smith, 2003), clearly linked to identities, but also demonstrating entitlement and including historical logs of transactions. A modern-day security specialist, of course, could list many technical flaws in these early token solutions. However, in their day, the measures probably matched the deviousness and resources of those that sought to undermine them. It is also worth remembering that some of the solutions involved additional human interaction and secondary checking. A well-recognized servant may have delivered the nobleman’s sealed letter, and the war time grocer would have known all his registered local customers and remembered their transactions. There is also the question of security priorities, for example, the servant delivering the sealed letter would probably have been less concerned about the risk of forgery, than that of being attacked by bandits.
22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

www.igi-global.com/chapter/smart-cards-security-assurance/25842?camid=4v1


www.igi-global.com/e-resources/library-recommendation/?id=1

Related Content

How do the Crowdfunders Judge the Crowdfunded?: Crowdfunding, Social Capital, and the Gatekeepers of the Financial Legitimacy
Mathieu-Claude Chaboud (2016). Strategic Approaches to Successful Crowdfunding (pp. 78-107).
www.igi-global.com/chapter/how-do-the-crowdfunders-judge-the-crowdfunded/141728?camid=4v1a

Reflecting on the Orchestra Metaphor: Aligning Business Models Simple Views
George Leal Jamil and Werner Silveira (2019). Handbook of Research on Business Models in Modern Competitive Scenarios (pp. 43-61).
www.igi-global.com/chapter/reflecting-on-the-orchestra-metaphor/219510?camid=4v1a

Carbon-Efficient Supply Chains
www.igi-global.com/article/carbon-efficient-supply-chains/134861?camid=4v1a
Audit Firms, Deferred Taxation and Financial Reporting: The Case of The Athens Stock Exchange
www.igi-global.com/article/audit-firms-deferred-taxation-and-financial-reporting/164984?camid=4v1a